Read Me First

Instructions and Guidance for RFC on the PCI KMO v1.0

PCI Security Standards Council

Introduction

First and foremost, the PCI Security Standards Council (PCI SSC) would like to thank you for taking the time to review **this draft of PCI KMO v1.0.**

Your review and feedback are fundamental to the ongoing evolution of our standards and programs. The following slides provide instructions and guidance that will assist you during your review.

Before You Begin

- **Please read these instructions and guidance in their entirety.**
- Plan your reviews ahead of time and ensure your feedback is submitted before the RFC period closes **at 11:59pm Eastern Time on 18 July 2025**.
- Refer to the What to Know Before Participating in a PCI SSC Request for Comment flyer for more information.

PCI Security Standards Council®

Purpose & Scope

The PCI SSC is planning a new standard that addresses key management operations across multiple other PCI standards. This new standard is the PCI KMO Standard.

As part of the planned revision effort, the PCI SSC is conducting an initial Request for Comment (RFC) period to solicit general feedback on the following document:

- *PCI Key Management Operations Security and Test Requirements*

This is an RFC on the first draft of the new PCI KMO Standard. Feedback received during this RFC period will be reviewed and considered for future RFC releases.

Note: *Revisions to existing standards and programs typically include RFCs on draft content. Given that this RFC is on a new Standard, at least one additional RFC is expected. Refer to the RFC Process Guide for more information.*

PCI KMO RFC Focus Areas

The PCI KMO Standard is intended to be referenced by other PCI standards and programs ("calling standard/program"). Examples of how this may work is provided in the "Example PCI KMO Implementations" and "Example Applicability Matrix" sections of the standard.

The goal for the initial release of PCI KMO is to address the key management operational requirements currently contained in the PCI PIN Standard and Domain 5 of the PCI P2PE Standard.

As the first RFC, it is expected the programmatic aspects of the PCI KMO Standard will continue to evolve based on changes to the test requirements. As such, the request for this RFC is to focus on the standard requirements themselves.

Example areas of the PCI KMO Standard that PCI SSC is soliciting input on include:

- Are the current requirements clearly and correctly stated?
- Are the current requirements sufficiently verifiable?
- Are any requirements missing, given the focus of PCI KMO on PCI PIN and PCI P2PE Domain 5?
- Are any requirements overly onerous or incorrectly addressing extant risk?

RFC Timeline

- The RFC period will run from **16 June 2025 to 18 July 2025.**
- Submit your feedback **before 11:59pm Eastern Time on 18 July 2025**.
- Late feedback **will not** be accepted.

Note: *PCI SSC can only accept feedback that is received via the Portal during the RFC period. Late feedback and feedback submitted via any other channel will not be accepted.*

RFC Feedback Instructions

PCI Security Standards Council

Accessing the RFC Document

Note: *Only your company's primary contact may log into the portal and download the RFC documents. If you do not know who your company's primary contact is, please contact RFC@pcisecuritystandards.org for assistance.*

- Log in to the PCI SSC Portal with your username and password: https://programs.pcissc.org/
  - *If you don't know your password, click "Forgot your password" to create a new password. If you do not have a username, please contact RFC@pcisecuritystandards.org for assistance.*
- Click on **RFC: PCI KMO v1.0**
- Accept the Non-Disclosure Agreement (NDA).
- Click to download the RFC document.

PCI Security Standards Council

Entering Your Feedback

1. In the *Document* field, choose one of the following options from the drop-down:
   - PCI KMO Security and Test Requirements v1.0

2. In the *Section* field, select or specify the appropriate document section that is the subject of your feedback (as applicable).

3. Specify the *Page Number* containing the content to which your feedback refers.

4. Select the appropriate *Category* of feedback from the drop-down menu.

5. Specify your *Comments* and provide a *Suggested Solution* for each item of feedback.

Note: *Further details describing the subject of your feedback should be specified in the Comments and/or Suggested Solution field(s).*

PCI Security Standards Council®

Maximizing Your Feedback

- In the Comment field, explain the reason for your feedback.
- In the Suggested Solution field, include a recommendation to address your feedback.
- Be as detailed as possible with your comments and suggested solutions.
- Feel free to leave either the Comment or Suggested Solution fields blank. It is not necessary to duplicate the same information in both fields.
- Do not submit the same feedback item more than once.
- Do not include company sensitive information and remember to keep your comments professional and collaborative.
- Consolidate all feedback for your company since each company can only provide 50 feedback entries.
- Please contact RFC@pcisecuritystandards.org with any questions or concerns.

PCI Security Standards Council

Other Feedback Reminders

- Ensure your work is saved after each entry and before you exit the portal, select “Save Draft Comments.”
- You can come back later to finish entering feedback; you do not need to enter all feedback in the same session.
- When all your feedback is complete, select “Submit Feedback” and then select “Ok” to confirm your submission is complete.
- Once you select “Ok,” you will not be able to edit your feedback.
- A confirmation email will be sent after you submit your feedback.
- All feedback received will be reviewed and considered by PCI SSC.

PCI Security Standards Council

After Submitting Your Feedback

- All RFC feedback will be reviewed and considered by PCI SSC.
- Your feedback, including your organization's name, and how PCI SSC actioned your feedback will be made available for review by RFC participants through the PCI SSC Portal.
- Refer to the PCI SSC RFC Process Guide for more information.

PCI Security Standards Council

Thank You!

PCI Security Standards Council®